EMAIL MANAGMENET

CRITICAL COMMUNICATION TOOL BUT ALSO THE MOST ATTACKED. HOW DO YOU MANAGE YOUR EMAIL SYSTEM?

1

INTRODUCTION – RYAN CAMRON

- 20 years of experience in IT between HealthCare, Hospitality and Government.
  Green County / 1100 Partners / Monroe Clinic/SSM Health / Marcus Hotels & Resorts
- Illinois Leadership Institute Board Member
- HIPAA Cow Security Group Co-Chair
- Green County Broadband Committee Chair
- GIPAW (Governmental Information Process Association of Wisconsin) Member
- NACo IT Committee Member
- County Mutual Cyber Resiliency Committee Member

2

AGENDA TOPICS

- OVERVIEW OF EMAIL SOCIAL ENGINEERING (PHISHING) EFFECTIVENESS
- EMAIL MANAGEMENT & SECURITY
  - EMAIL EDUCATION & AWARENESS TRAININGS FOR STAFF
  - EMAIL POLICIES TO PROTECT YOUR ORGANIZATION & STAFF
  - EMAIL ENCRYPTION
  - EMAIL DATA LOSS PREVENTION
  - EMAIL ARCHIVING

3

EMAIL: WHAT IS SOCIAL ENGINEERING?

SOCIAL ENGINEERING – SOCIAL ENGINEERING IS THE ART OF MANIPULATING PEOPLE INTO PERFORMING ACTIONS OR DIVULGING CONFIDENTIAL INFORMATION. TYPICALLY THE ATTACKER NEVER COMES FACE TO FACE WITH THE VICTIMS.

4

EMAIL: TYPES OF SOCIAL ENGINEERING EMAIL SCAMS

Image from Fortinet.com

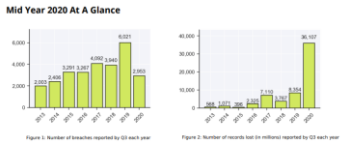
5

EMAIL: IS SOCIAL ENGINEERING REALLY EFFECTIVE?

- 96% of all social attacks arrive via email – 2020 Verizon Data Breach Investigations Report
- 91% of all success data breaches start with a spear phishing email attack – knowbe4
- 95% of breaches involved human error – 2020 Verizon Date Breach Investigations Report
- 90% of all healthcare organizations reported at least one security breach in the last three years – Becker's Hospital Review

6

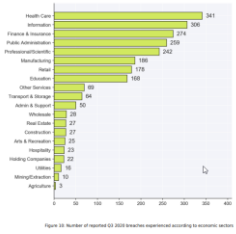
EMAIL: IS SOCIAL ENGINEERING REALLY EFFECTIVE?



Risk Based Security Group Q3 2020 Report

7

EMAIL: IS SOCIAL ENGINEERING REALLY EFFECTIVE?



Risk Based Security Group Q3 2020 Report

8

EMAIL: SO HOW DO WE PROTECT/MANAGE EMAIL

1. Education / Awareness Training
2. Effective Policies
3. Encryption for Emails
4. Data Loss Prevention (DLP) Software
5. Archiving Software

9

EMAIL: EDUCATION & AWARENESS TRAININGS

10

EMAIL: WHEN SHOULD YOU DO EDUCATION & AWARENESS TRAININGS

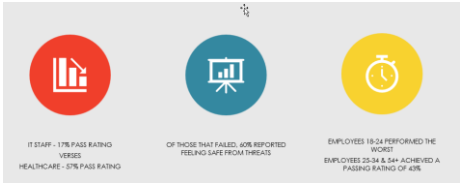
- New Employee Orientations – Work with your Administration and Human Resources to get 15 to 30 minutes during new employee orientations. Educating staff as soon as they start will drive compliance and reduce risks.
- Annual Awareness Sessions – Schedule lunch & learn type of events to continue educating staff.
- Periodic phishing email campaigns – Just at least be annually to gauge where your staff are at and how effective your trainings are.

** Our jobs/positions require continued education/training. Email security awareness should be the same.**

11

EMAIL: PHISHING CAMPAIGN FUN FACT

- 2020 Phishing Campaign Survey Results – Data Collected from organizations cross the US by Knowbe4



12

EMAIL:WHAT'S THE BASIS FOR A GOOD TRAINING?

- Phishing Campaigns – Make them realistic and relevant to what is actively happening either locally or nationally. Make sure that the program is not designed to be punitive!
- Make the information relevant to not only the business but how they can apply to their personal lives.
- Make it interactive! Get your audience engaged.
- Keep it SIMPLE!

13

EMAIL:TRAINING EXAMPLES

- Making it relevant to your audience -

Cyber-Security Aligns With Infection Control

Once a virus enters the human body, it looks for an acceptable host cell. Once a computer virus enters the Network, it looks for an acceptable host computer.

Computer World	Biological World
Computer	Human body
Malware execution	Virus replication
Anti Virus Analyst	Medical Doctor
Anti Virus system	Immune system
Firewall	External barriers
USB, Bluetooth..	Cough, fluids...

14

EMAIL:TRAINING EXAMPLES

- Making it relevant to your audience -

Everyone is a defender against cyber attacks!

Security Technology will never be 100% in preventing infections, just as **vaccines** will never be 100% in preventing biological infections.

Reactive – Security Technology & Vaccines (based on historical data & best guess on what will happen)

Proactive – Humans! (Most Critical Part of Security)

15

EMAIL:TRAINING EXAMPLE

- Making it Interactive

16

EMAIL:TRAINING EXAMPLE

- Engaging staff – What's wrong with this email?

From: Mary Mezera <reply@sendmailsoutlook.com>
Sent: Thursday, April 7, 2022 7:31 PM
To: Traci Kubly <tkubly@gchcd.org>
Subject: Aging Report Request

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hi Traci,

Send me the Aging report from A/R and include each customer payable contact emails on this report.

How soon can you get it done?

Thanks,
Mary

17

EMAIL: POLICIES – THAT SHOULD INCLUDE EMAIL!

- Mobile Device Management – Do you have a mobile device policy? (applies even if you don't have an MDM software). Remember, most people are accessing email on their phones.
- Auditing Policy – Do you have a policy that covers when/how audits are performed?
- Disaster Recovery Policy – Does your DR policy include email? If it doesn't it should!
- Retention Policy – Do you have a retention policy for emails?
- Risk/Management Policy – Do you cover emails within your risk/mgmt. policy?
- Acceptable Use Policy – Does your acceptable use policy cover email?

18

EMAIL: ENCRYPTION

What is Email encryption? Emails encryption entails securing an email from the point of sender to the point of the receiver.

Why do we need this? Encrypting an email is the way to make sure that it is secure. Normal email sent without encryption is done in plain text.

Plain text means that if someone were to intercept the email while in transit, they could read the entire message.

While encrypting a message locks the message and they only way to see the contents is by having the key to open it.

19

EMAIL: ENCRYPTION

- Each organization is different on how this is handled but here are two ways
  - Automatic encryption (TLS – Transport Layer Security))done by the email system (reliant on the other end also having TLS configured) other wise sent out as plain text.
  - Staff Manually encrypting messages – Typing a specific word into the subject line of an email. Examples: SECURE:, SECURE!, etc. Refer to your IT department for more information.

20

EMAIL: DATA LOSS PREVENTION (DLP)

- What is DLP?

  Data Loss Prevention is a tool that monitors and protects business data from unauthorized access. When implemented is protects in three places: authorized personnel, in motion (being transferred via the internet) or while at rest (in a file or database).

  There are three types of DLP:

  Endpoint – Looks at all data on a computer

  Cloud – Looks at data that a user has in the cloud.

  Network – Looks a data traversing the network, like email!

21

EMAIL: DATA LOSS PREVENTION (DLP)

- How does it work?

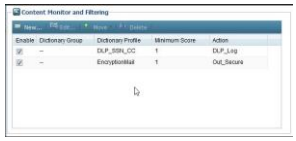
  DLP works by examining the contents of data for common characteristics that you predefine.

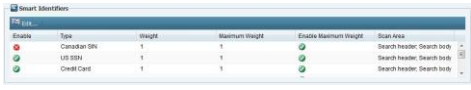
  Rules can be as simple or complex as your organization deems necessary to secure data.

22

EMAIL: DATA LOSS PREVENTION (DLP)

- Examples:





23

EMAIL: CONTACT INFORMATION

- RYAN CAMRON
- EMAIL: RCAMRON@GREENCOUNTYWI.ORG
- PHONE: 608-328-9348

24

REFERENCES

- Risk Based Security Report: https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf
- Phishing Box: https://www.phishingbox.com/resources/social-engineering-attacks
- 2021 DBR Report: https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2021.pdf
- NIST Phish Scale: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=931366

25